

⑥

AN UNDETERMINED MATRIX  
MOMENT PROBLEM AND ITS  
APPLICATION TO COMPUTING  
ZEROS OF L-FUNCTIONS

PETER SARNAK  
(JOINT WITH M. RUBINSTEIN)

SIMONS INSTITUTE  
BERKELEY

FEB 2019

①

## COMPLEXITY OF COMPUTING ZEROS

$\pi$  AN AUTOMORPHIC CUSP FORM  
ON  $GL_m / \mathbb{Q}$  ( $m=2$ ).

$L(s, \pi)$  ITS STANDARD L-FUNCTION

$L(s, \pi_p)$  = LOCAL FACTOR AT  $p$

$$L(s, \pi) = \prod_{p < \infty} L(s, \pi_p)$$

$$\Lambda(s, \pi) = L(s, \pi_\infty) L(s, \pi)$$

ANALYTIC CONTINUATION AND FUNCTIONAL EQ<sup>n</sup>:

$$\Lambda(1-s, \pi) = w(\pi) N_\pi^{s-1/2} \Lambda(s, \pi)$$

$\pi = \tilde{\pi}$  (ASSUMPTION) SELF DUAL

$w(\pi) = \pm 1$  : ROOT NUMBER

$N_\pi$  IS THE CONDUCTOR, IT IS A  
PRODUCT OVER PRIMES AT WHICH  $\pi$  IS  
RAMIFIED.

$N_\pi$  MEASURES THE COMPLEXITY OF  $\pi$  ;  
WANT TO COMPUTE ZEROS OF  $L(s, \pi)$  NEAR  $1/2$ .

# EXPLICATE WITH ELLIPTIC CURVES

[2]

WEISTRASS FORM:

$$E: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad (1)$$

$a_j \in \mathbb{Z}$ . CORRESPONDING INVARIANTS ARE

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1 a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6, \quad b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$$

$$C_4 = b_2^2 - 24 b_4 \quad C_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6$$

$$\text{DISCRIMINANT} \quad \Delta = -b_2^2 b_8 - 8 b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6$$

—(2)

WE ASSUME THAT  $(C_4, C_6) = 1$  AND  $(C_4, 6) = 1$  SO THAT E HAS ONLY MULTIPLICATIVE BAD REDUCTION

$\Rightarrow N_E$  THE CONDUCTOR OF E IS SQUARE FREE PART OF  $|\Delta|$ , ASSUME LATTER IS SQ. FREE.

$$N_E = |\Delta|$$

$$W(E) = -\left(\frac{C_6}{N_E}\right) \mu(N_E) ;$$

$\mu$  THE MOBIUS FUNCTION THE PARITY OF THE NUMBER OF PRIME FACTORS.

THE ORDER OF VANISHING OF  $L(S, E)$  AT  $s = 1/2$  IS THE RANK OF  $E/\mathbb{Q}$  (BSD).

• ONE CAN COMPUTE  $L(s, E_p)$  THE LOCAL <sup>(3)</sup>  
FACTOR AT  $p$  IN  $\text{POLY LOG}(p)$  STEPS (SCHOOF)

$$\Rightarrow L(s, E) = \sum_{n=1}^{\infty} \lambda_E(n) n^{-s}$$

THEN FOR ANY  $\epsilon$  WE CAN COMPUTE  
THE  $\lambda_E(n)$ 'S  $\wedge$  IN  $\epsilon^{1+o(1)}$  STEPS.

RIEMANN'S GOLD STANDARD :

GIVEN  $W(E)$ , USING THE "APPROXIMATE  
FUNCTIONAL EQUATION" (RIEMANN -  
SIEGEL FORMULA) ONE CAN COMPUTE  
 $L(s, E)$  FOR  $s$  NEAR  $1/2$  IN

$N_E^{1/2+o(1)}$  STEPS.

$W(E)$  IS A PRODUCT OVER  $p$ 'S DIVIDING  
 $N_E$  OF  $W_p(E)$ , SO  $W(E)$  CAN BE COMPUTED  
IN  $N_E^{1/2}$  STEPS TRIVIALY.

⇒ ONE CAN COMPUTE THE COUNTING FN. 4

$$S(E, t) = \# \left\{ \rho = \frac{1}{2} + i\gamma : 0 \leq \gamma \leq t, L(\rho, E) = 0 \right\} \quad (4)$$

AND IN PARTICULAR THE RANK IN

$N_E^{1/2 + o(1)}$  STEPS.

CAN ONE DO BETTER; BREAK THE  $1/2$  BARRIER, OR EVEN  $N_E^{o(1)}$  STEPS I. E. SUBEXPONENTIAL.

### THE ELUSIVE PARITY:

THE PARITY OF THE NUMBER OF PRIME FACTORS OF A NUMBER IS ONE OF ITS BEST KEPT SECRETS. THEORETICALLY IN SIEVE THEORY THERE IS THE WELL KNOWN SIEVE LIMIT ON RECOGNISING PARITY. COMPUTATIONALLY AS FAR AS WE KNOW THE FASTEST WAY TO COMPUTE  $\mu(N)$  IS TO FACTOR  $N$  - AND THESE ARE PROBABLY OF THE SAME COMPLEXITY. THE BEST FACTORING ALGORITHMS ARE SUBEXPONENTIAL IN  $N$ , AND GIVE BENCH MARKS FOR OUR PROBLEM.

THEOREM (RUBINSTEIN/S) :

ONE CAN COMPUTE  $W(E)$  (WITHOUT FACTORING  $N_E$ ) AND  $S(E, t)$  FOR MANY  $t$ 's, IN SUBEXPONENTIAL TIME.

REMARKS:

(A) WE ARE ASSUMING GRH THROUGHOUT.

(B) THE ALGORITHM WHEN IT TERMINATES GIVES CORRECT ANSWERS. THE FACT THAT IT DOES TERMINATE QUICKLY DEPENDS ON CONJECTURES (KATZ/S) RELATING THE DISTRIBUTION OF THE ZEROS TO RANDOM MATRIX ENSEMBLES.

THE BASIS OF THE COMPUTATION IS THE EXPLICIT FORMULA OF RIEMANN, GUINAND, WEIL :

$\phi \in \mathcal{S}(\mathbb{R})$ ,  $\hat{\phi}$  F.T  $\hat{\phi}$  COMPACT SUPPORT

$\phi$  EVEN

$\frac{1}{2} + i\gamma = \rho$  THE ZEROS OF  $\zeta(s, \pi)$

$$\sum \phi(\gamma) = \frac{\hat{\phi}(0)}{\pi} \log N_{\pi} + \frac{1}{\pi} \int_{-\infty}^{\infty} \phi(t) \operatorname{Re} \left( \frac{L'(\frac{1}{2} + it, \pi)}{L_0(\frac{1}{2} + it, \pi)} \right) dt - \frac{1}{\pi} \sum_{n=1}^{\infty} \frac{c(n)}{\sqrt{n}} \hat{\phi} \left( \frac{\log n}{2\pi} \right)$$

WHERE  $L'/L(s, \pi) = - \sum_{n=1}^{\infty} \frac{c(n)}{n^s}$

IF WE COMPUTE  $c(n)$  FOR  $n \leq x$ , BY LIMITING SUPPORT  $\hat{\phi}$ , THE ABOVE IS A SYSTEM OF EQUATIONS FOR THE  $\gamma$ 'S.

THIS SYSTEM REDUCES TO THE FOLLOWING BASIC PROBLEM WITH

$$\log N_{\pi} \approx \pi$$

UNDERDETERMINED MOMENT PROBLEM

$O(2n+1)$  ORTHOGONAL GROUP SIZE  $2n+1$

FOR  $A \in O(2n+1)$

$$P_A(\lambda) = \det(\lambda I - A) = \lambda^{2n+1} + a_1 \lambda^{2n} + \dots + a_{2n} \lambda + a_{2n+1} \quad (4)$$

$$a_{2n+1} = -\det A, \quad a_j = -(\det A) a_{2n+1-j}$$

SINCE  $\lambda^{2n+1} P_A(\lambda^{-1}) = (\det A) P_A(\lambda)$  SELF RECIPROCAL

WE ARE GIVEN THE FIRST  $k$ -MOMENTS

$$S_j(A) = \text{trace}(A^j), \quad 0 \leq j \leq k$$
$$= (\det A)^j + \sum_{\nu=1}^n 2 \cos(j \theta_{\nu}) \quad (5)$$

HERE THE  $2n+1$  EIGENVALUES OF  $A$  ARE  $\det A, e^{i\theta_1}, e^{-i\theta_1}, \dots, e^{i\theta_n}, e^{-i\theta_n}$



• IF  $k=n$  AND  $\det A = \pm 1$  IS  $\textcircled{8}$   
KNOWN THEN (4) AND (5) AND NEWTON  
GIVE THE  $q_j$ 's FOR ALL  $j$  AND HENCE  $\theta_j$ 's.

• OUR L-FUNCTION PROBLEM ONCE WE  
HAVE COMPUTED THE  $C(n)$ 's FOR  
 $n \in \mathbb{N}_\pi^\alpha$ , REDUCES TO (5) WITH

$$\frac{k}{n} = 2\alpha \quad \text{--- (6)}$$

SO  $\alpha = \frac{1}{2}$  (RIEMANN'S GOLD STANDARD)  
CORRESPONDS EXACTLY TO  $k=n$   
WHEN EVERYTHING CAN BE COMPUTED.

COMPLEXITY  $\alpha < \frac{1}{2}$  YIELDS THE  
CORRESPONDING UNDERDETERMINED PROBLEM:

GIVEN  $y \in \mathbb{R}^k$ ,  $y = (s_1, s_2, \dots, s_k)$   
OUR GIVEN MOMENTS WHAT CAN WE  
SAY ABOUT  $\det A$  AND THE  $\theta_j$ 's ?

## FORBIDDEN SET $F(y)$ :

19

LET  $F(y) \subset [0, \pi]$  BE THE SET OF  $t$ 's WHICH ARE NOT THE EIGENVALUES OF ANY  $A$  WHOSE FIRST  $k$ -MOMENTS ARE  $y$ .

• IF  $F(y)$  IS LARGE WE LEARN SOMETHING ABOUT THE EIGENVALUES — THEY ARE RESTRICTED TO LIE IN THE UNION OF INTERVALS WHICH FORM THE ADMISSIBLE SET

$$G(y) = [0, \pi] \setminus F(y)$$

• IF  $k < n$ ,  $F(y)$  MAY BE EMPTY FOR EXAMPLE IF THE  $\theta$ 's LIE ON AN ARITHMETIC PROGRESSION, BUT FOR TYPICAL  $y$  AND  $\alpha$  NOT TOO SMALL THIS WON'T HAPPEN.

## EXACT COUNT SET $E(y)$ :

$E(y)$  CONSISTS OF ALL  $t$ 's IN  $[0, \pi]$  FOR WHICH THE NUMBER  $J_y(t)$  OF EIGENVALUES  $\theta_1, \theta_2, \dots, \det A$ , LIE IN  $[0, t]$  IS DETERMINED INDEPENDENT OF  $A$ .

$$E(y) \subset F(y)$$

110

HOW TO COMPUTE THESE EFFICIENTLY  
AND WHAT DO THEY LOOK LIKE AS  
A FUNCTION OF  $\alpha = k/n$  ?

MOMENT CURVE:

CLOSELY RELATED TO THE ABOVE IS  
THE MOMENT CURVE;  $t = \cos \theta$   
 $-1 \leq t \leq 1$

$$M: [-1, 1] \rightarrow \mathbb{R}^k; M(t) = (t, t^2, \dots, t^k)$$

$$C := M([-1, 1]) \subset \mathbb{R}^k$$

FOR  $n \geq 1$  (OUR INTEREST IS  $n > k$ )

$$A(k, n) := \underbrace{C + C + C \dots + C}_{n \text{-times}} \subset \mathbb{R}^k$$

BASIC COMPLEXITY PROBLEM:

III

FOR  $\exists \in \mathbb{R}^k$  IS  $\exists \in A(k, n)$ ?

DOES THIS HAVE AN EFFICIENT SOLUTION (IE POLYNOMIAL TIME)?

• NOTE THAT FOR  $A(k, k)$  IT DOES SINCE IN THIS CASE WE GET THE FULL CHARACTERISTIC POLYNOMIAL AND HENCE RECOVER THE ROOTS EFFICIENTLY.

BUT HOW ABOUT  $n = 2k$ ?

RELEVANCE: TO COMPUTE  $F(y)$  WE CONSIDER FOR EACH  $t \in [-1, 1]$  WHETHER

$$y - M(t) \in A(k, n-1)$$

THIS IS SO IFF  $t \in F(y)$ .

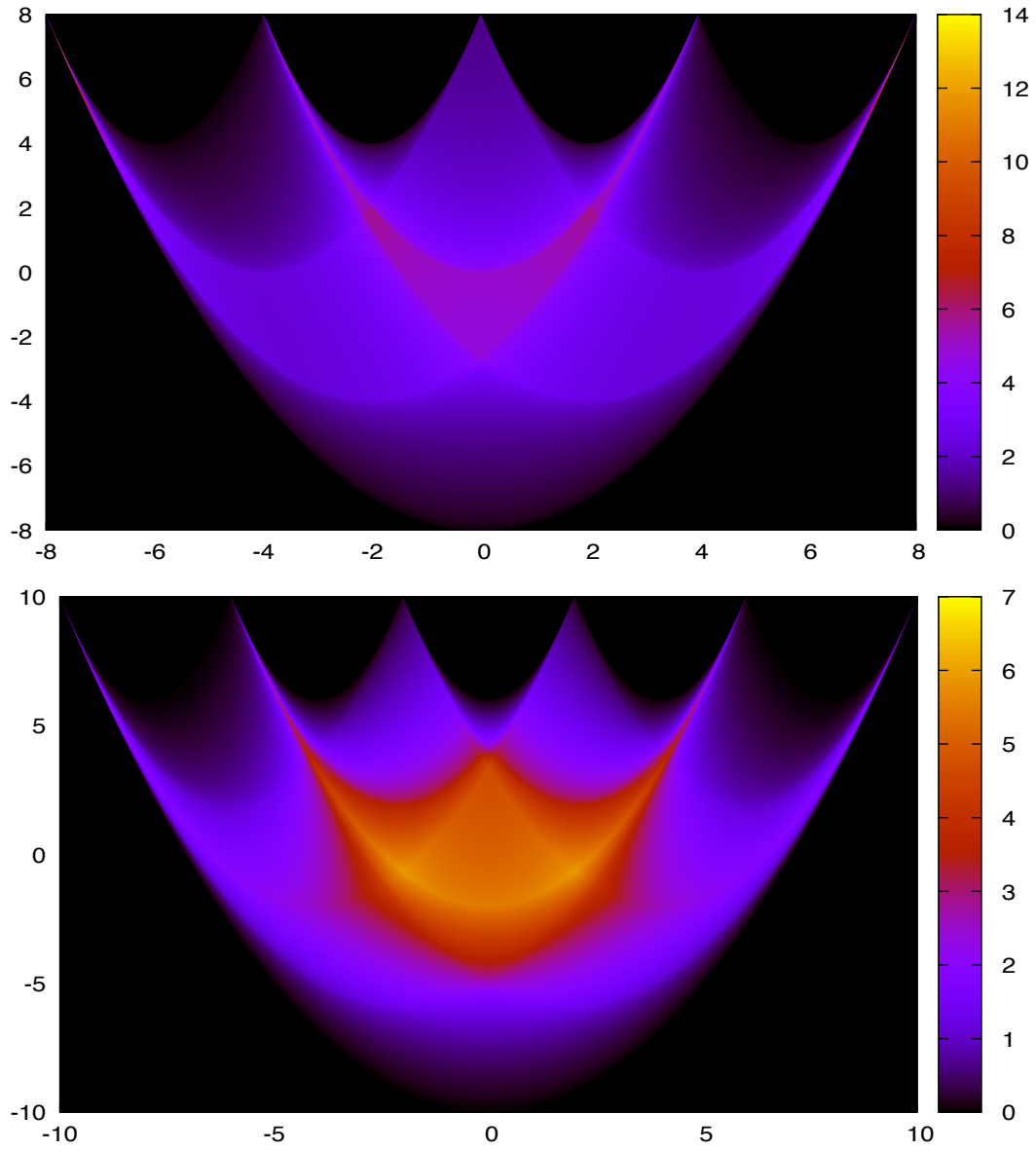


FIGURE 4. Heat maps depicting the distribution of points in the sets  $A(2, 4)$ ,  $A(2, 5)$ .

Then, for  $u = c(t_1) + c(t_2) + \dots + c(t_k) \in A(k, n)$ ,

$$(9) \quad v(u) = \sum_{j=1}^n f(t_j).$$

Hence  $v(u) \leq 0$  for all  $u \in A(k, n)$  iff  $f(t) \leq 0$  for all  $t$ .

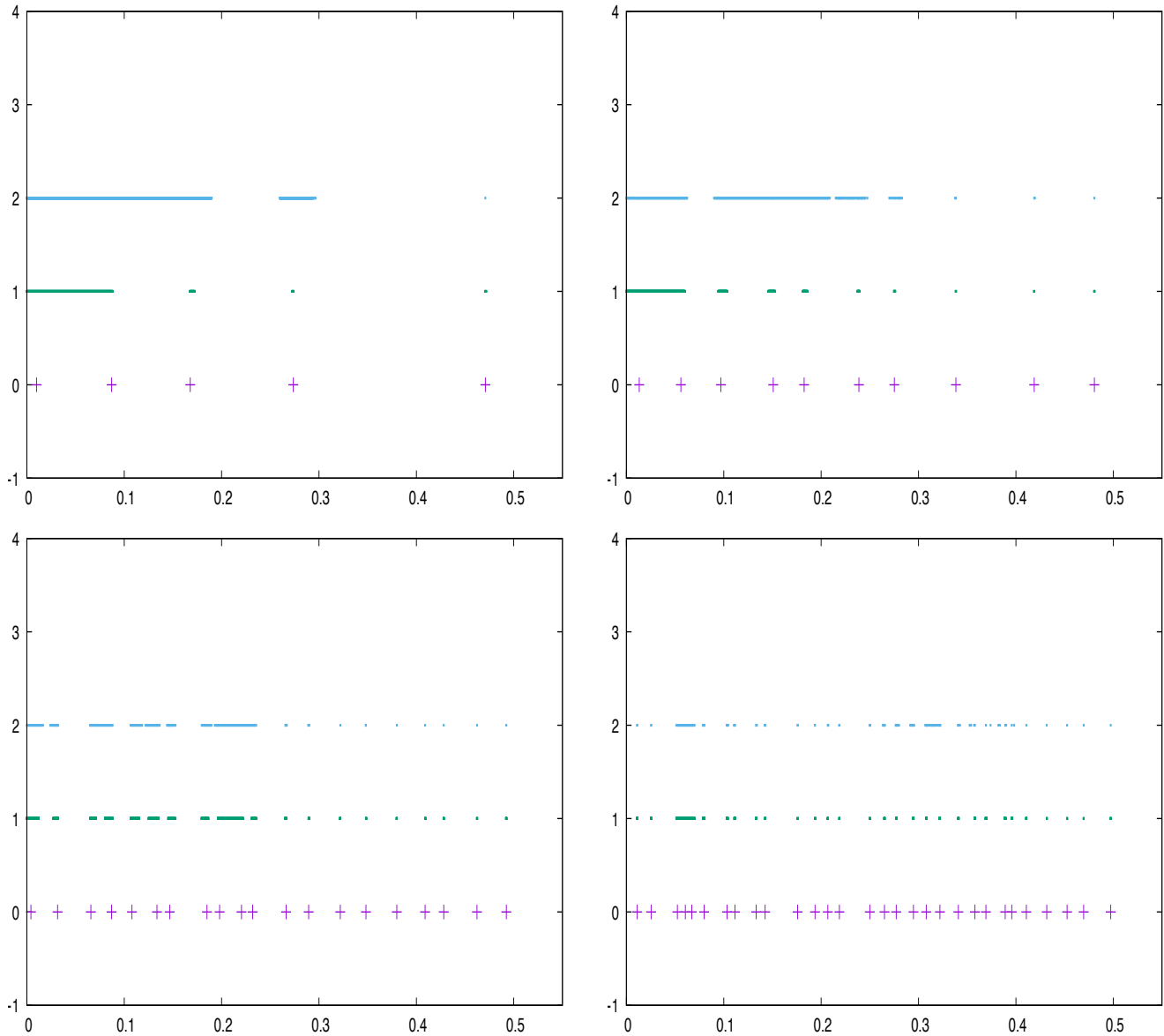


FIGURE 1. Plots depicting the admissible sets (i.e. complement of  $F(y)$ ), for 2 Haar sampled matrices in  $SO(2n)$ , with  $n = 5, 10, 20, 30$ , and  $k = n - j$ , with  $j = 0, 1, 2$ . The horizontal depicts the points  $t \in [0, 1/2]$  in the admissible set, while the vertical axis is  $j$ . ( $j = 2$  needs to be redrawn to higher resolution. will include  $n = 5, 30$  later today)

OUR (EFFICIENT) ALGORITHM INVOLVES AN ITERATIVE CONVEXIFICATION OF THE BASIC PROBLEM COUPLED WITH A SECOND LINEAR PROGRAM.

IT YIELDS (GOOD IN TYPICAL SITUATIONS) LOWER BOUNDS FOR  $F(y)$  AND  $E(y)$ .

MORE GENERALLY; FOR  $G(y) \in [-1, 1]$  LET

$C_G = M(G) \subset \mathbb{R}^k$  AND

$A_G(k, n) = C_G + C_G + \dots + C_G$

OUR INTEREST IS  $G$  A UNION OF INTERVALS (FINITELY MANY)

THE QUESTION OF WHETHER  $\exists \in \mathbb{R}^k$  IS IN  $A_G(k, n)$  IS ALREADY HARD SINCE FOR  $k=1$  AND  $G$  SAY  $n$  POINTS, IT CONTAINS THE SUB-SUM PROBLEM WHICH IS NP COMPLETE (KARP)

WE RELAX THE PROBLEM TO DETERMINE IF  $\exists$  IS IN THE CONVEX HULL OF A:

$\exists \notin CH(A_G(k, n))$  IFF THERE IS A SEPARATING HYPER PLANE

$$\min_b (b_0 + b_1 \beta_1 + \dots + b_k \beta_k) < 0 \quad \left. \right\} \text{LP1}$$

SUBJECT TO  $b_0 + b_1 t + \dots + b_k t^k \geq 0$  FOR  $t \in G$

FOR EXACT COUNTING  $J \subset [-1, 1]$  INTERVAL

$y \in \mathbb{R}^k$ , ESTIMATE

$$S_y(J) = \# \sum \theta \text{'s, det } A \text{ in } J : M(A) = y \}$$

$$\pi b_0 + \dots + b_k y_k = L(y) \leq S_y(J) \leq U(y) = n c_0 + c_1 y_1 + \dots + c_k y_k$$

SATISFYING:  $\sum_{j=0}^k b_j t^j \leq \chi_J(t) \leq \sum_{j=0}^k c_j t^j ; t \in J \cap G$

LINEAR PROGRAM

$$\Delta_y(J) = \min_{b, c} [U(y) - L(y)] \quad \left. \right\} \text{LP2}$$



• IF  $\Delta_y(J) < 1$  THEN  $S_y(J)$   
WHICH IS AN INTEGER IS DETERMINED!

### ITERATION:

INITIALIZE  $G = [-1, 1]$

FOR EACH  $t \in [-1, 1]$  RUN LP1 TO  
CHECK IF  $y - M(t) \in CH(A(k, n-1))$

IF NOT  $t \in F_1(y)$ .

FOR EACH  $t \in F_1(y)$  RUN LP2  
TO OBTAIN  $E_1(y)$  WHEN  $S_y([-1, t])$  IS  
DETERMINED.

ITERATE:  $G_2(y) = [-1, 1] \setminus F_1(y)$ ,

...  $F_2(y), G_2(y), E_2(y), \dots$

$$F_1(y) \subset F_2(y) \dots F_\infty(y) \subset F(y)$$

$$E_1(y) \subset E_2(y) \dots E_\infty(y) \subset E(y)$$

$$S_y(t) \quad t \in E_\infty(y)$$

NB: AT THE FIRST STEP  $G = [-1, 1]$  15  
 LP1 AND LP2 HAVE EXPLICIT SOLUTIONS  
 BY HAMBURGER, CHEBYSHEV AND MARKOV.  
 WE USE THESE AT THIS STEP AND IT  
 ALSO IS IMPORTANT FOR ANALYSIS

THEOREM:  $\xi \in \mathbb{R}^k$  IS IN  $CH(C)$

IFF THE HANKEL MATRICES

$$k=2v$$

$$\left( \xi_{i+j} \right)_{\substack{i=0,1,\dots,v \\ j=0,1,\dots,v}}$$

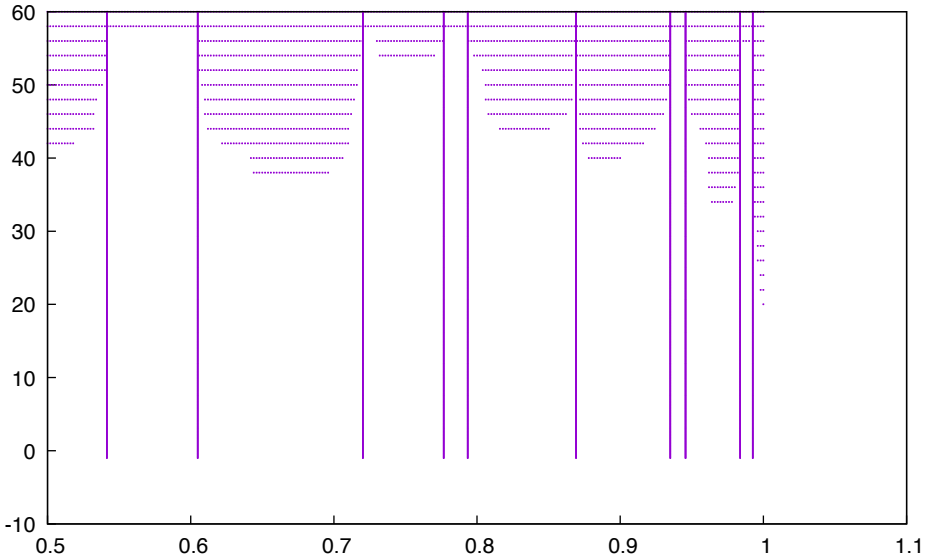
$$\xi_0 = 1$$

AND

$$\left( 2\xi_{i+j+1} - \xi_{i+j} - \xi_{i+j+2} \right)_{\substack{i=0,1,\dots,v-1 \\ j=0,1,\dots,v-1}}$$

ARE NONNEGATIVE.

THE SOLUTION OF LP2 FOR  $G = [-1, 1]$   
 BY CHEBYSHEV AND MARKOV USES THEIR  
 THEORY OF NODES AND WEIGHTS  
 (VIA PADE APPROXIMATIONS)



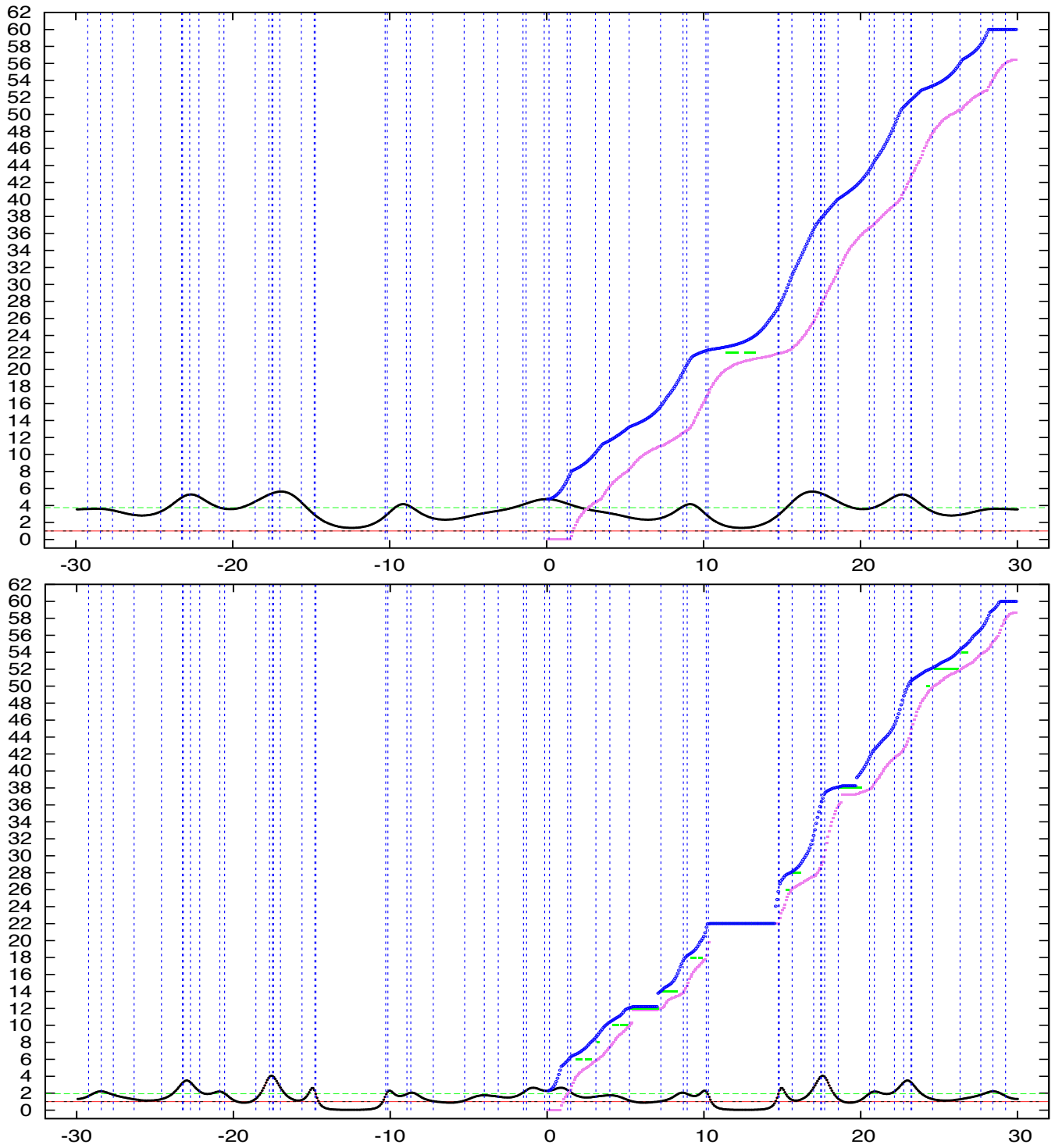


FIGURE 6. The same as the previous figure, but for 30 pairs of zeros, symmetric about 0, chosen uniformly and independently at random, for  $k = 15$  (top) and  $k = 30$  (bottom). We notice that there are larger gaps (as well as many smaller gaps) in comparison to the  $SO(60)$  example, and that more of the gaps are detected sooner.

•  $F_1(y)$  MAY BE EMPTY IN WHICH 116  
CASE WE LEARN NOTHING.

THE KEY POINT THAT WE ESTABLISH IS THAT IF

$2\alpha = k/m$  GOES TO 0 SLOWLY  
THEN BOTH  $F_1(y)$  AND  $E_1(y)$   
ARE NON EMPTY (IN FACT QUITE  
LARGE) IF  $y = M(A)$  IS DRAWN  
AT RANDOM W.R.T. HAAR MEASURE  
ON  $O(2n+1)$ .

• NOTE THAT ONCE  $E_\infty(y) \neq \emptyset$   
AND  $-1 < t < 1$  IS IN  $E_\infty(y)$  THEN  
THE PARITY OF  $S_y(t)$  IS EVEN  
IFF  $\det A = 1$ , THAT IS WE  
DETERMINE  $W(A)$

$\Rightarrow$  SUBEXPONENTIAL COMP. OF  $W(E)$ .

WHAT IS THE LIMIT OF 17  
THIS METHOD — HOW SMALL CAN  
 $k/n$  BE FOR  $W(A)$  TO BE COMPUTED?

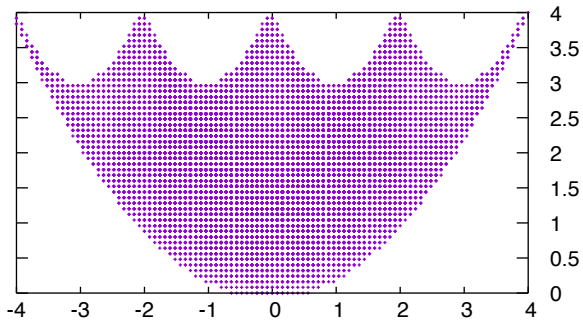
A LIMIT IS SET BY THE VERY STRONG  
Szego LIMIT TYPE THEOREM OF  
JOHANSSON / LANIBERT (2019):

LET  $\nu_+(k, n), \nu_-(k, n)$  BE THE  
PUSH FORWARD MOMENT MEASURES  
(ON  $\mathbb{R}^k$ ) OF HAAR MEASURE ON  
 $O^+(2n+1)$  AND  $O^-(2n+1)$ . THEN FOR  
 $k = n^\alpha, 0 \leq \alpha < 1/3$   
TOTAL VARIATION  $[\nu_+(k, n), \nu_-(k, n)] \leq C e^{-c(1-\alpha)n^{1-\alpha}}$

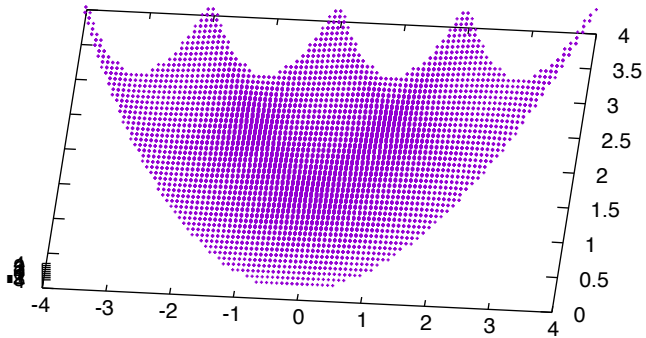
---

SO CERTAINLY THERE IS NO  
POLYNOMIAL TIME COMPUTATION OF  
 $W(N_E)$  BY THIS METHOD.

"A\_3\_4\_new"

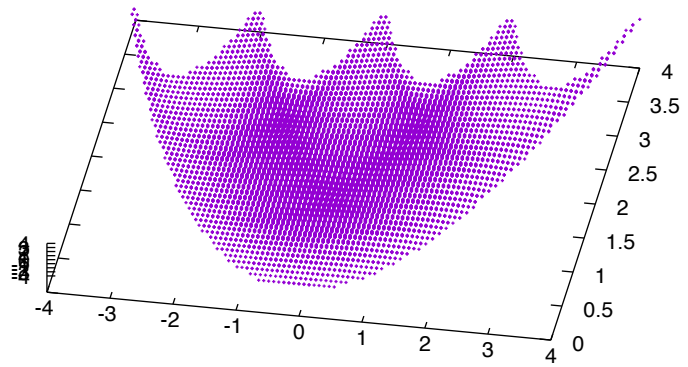


"A\_3\_4\_new" .

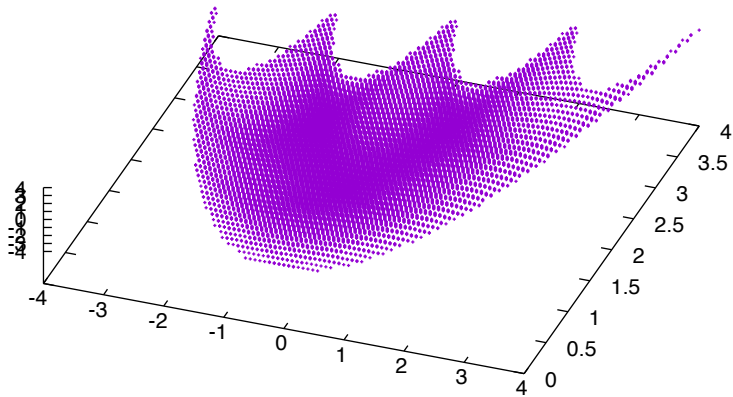




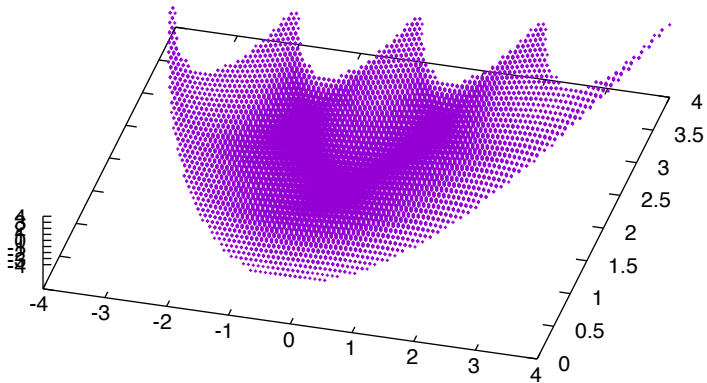
"A\_3\_4\_new" ·



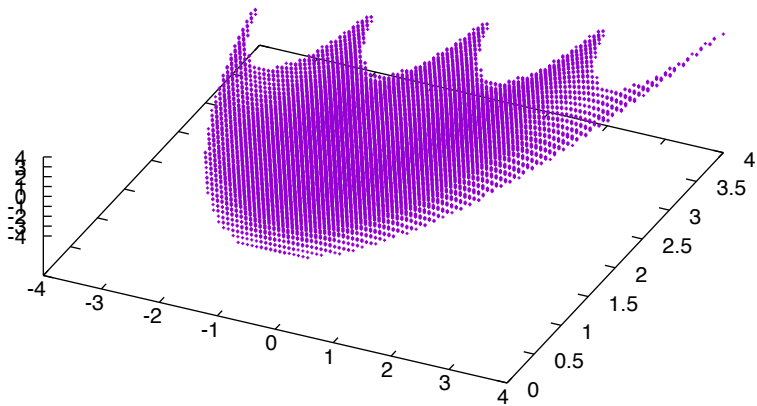
"A\_3\_4\_new" .



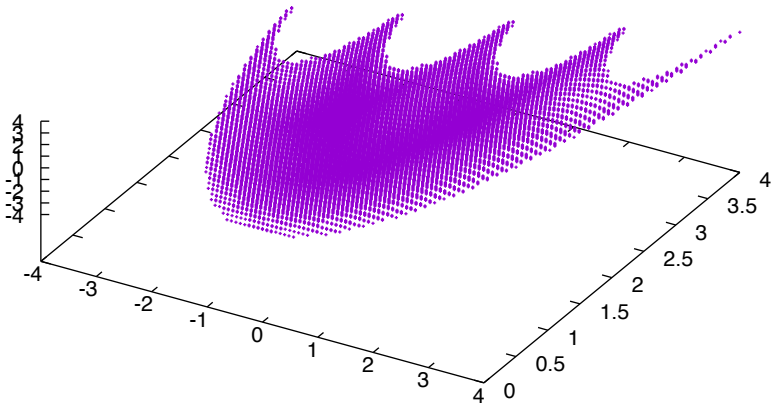
"A\_3\_4\_new" ·



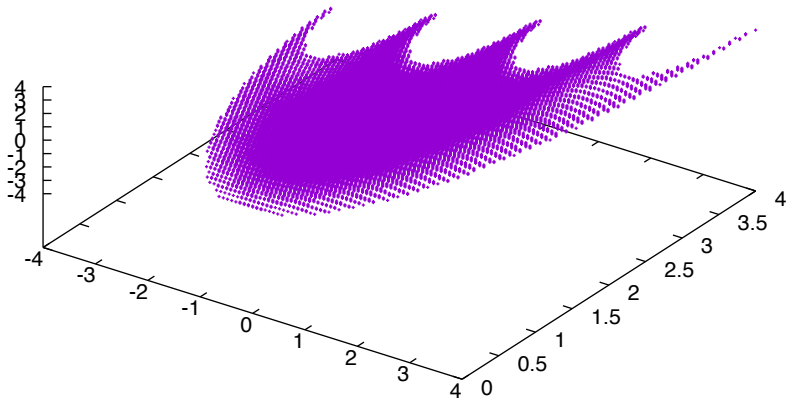
"A\_3\_4\_new" .



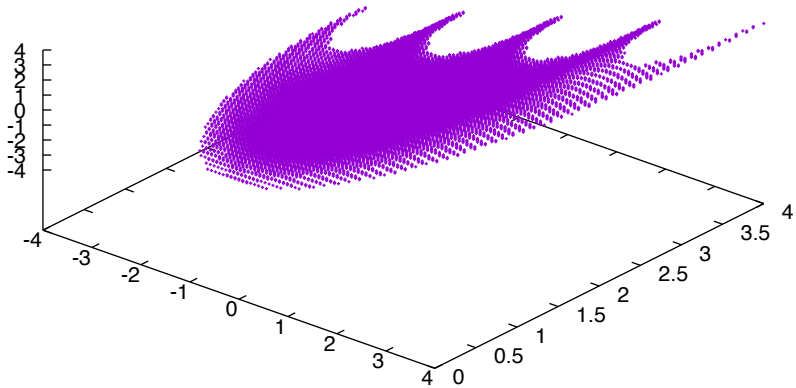
"A\_3\_4\_new" .



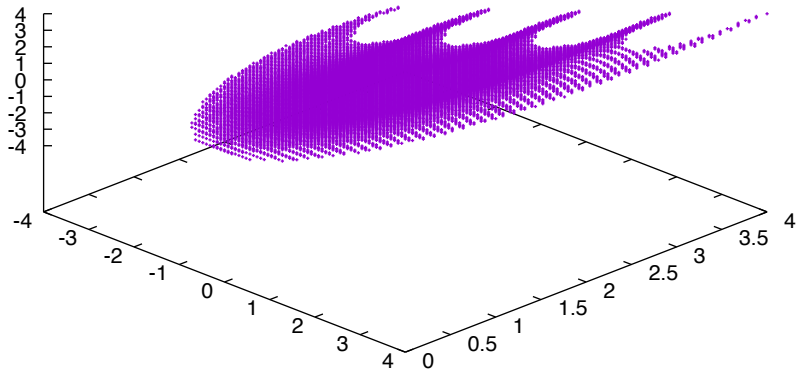
"A\_3\_4\_new" ·



"A\_3\_4\_new" .

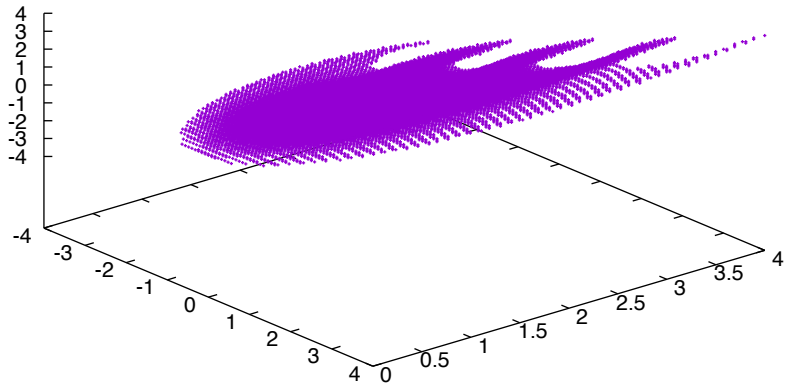


"A\_3\_4\_new" .

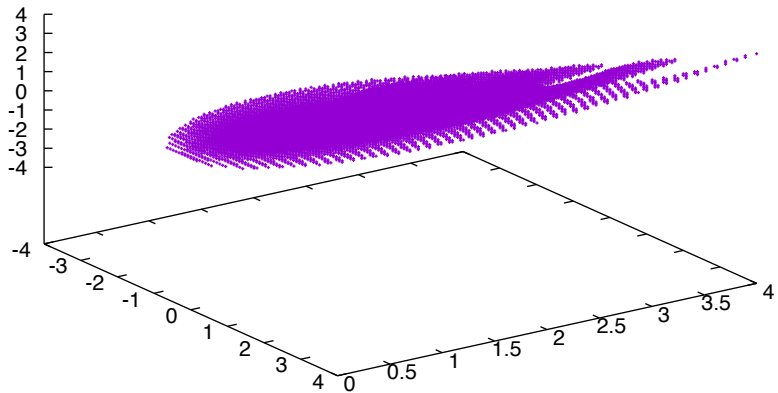




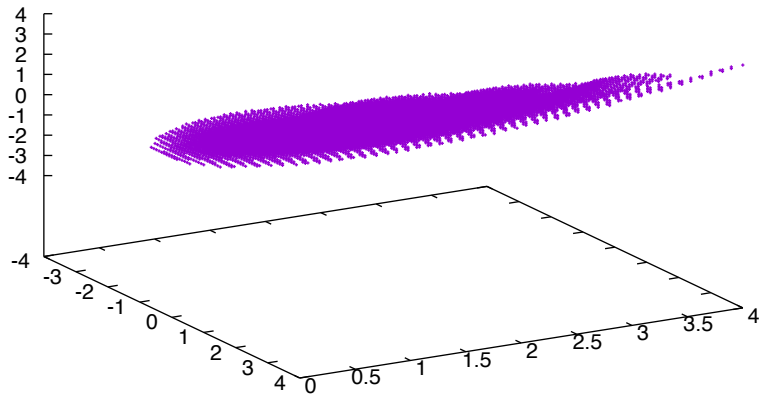
"A\_3\_4\_new" .



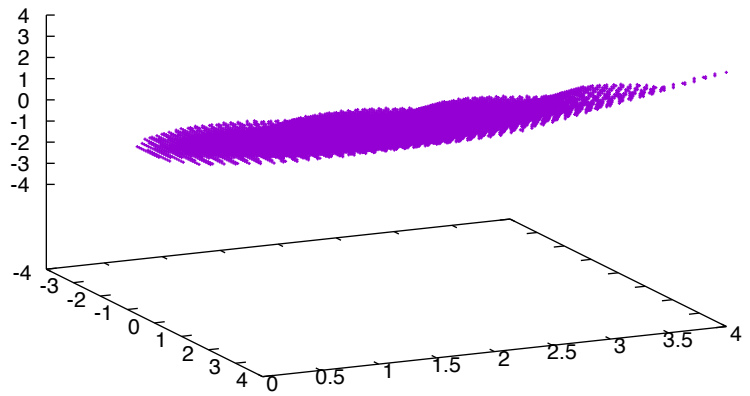
"A\_3\_4\_new" .



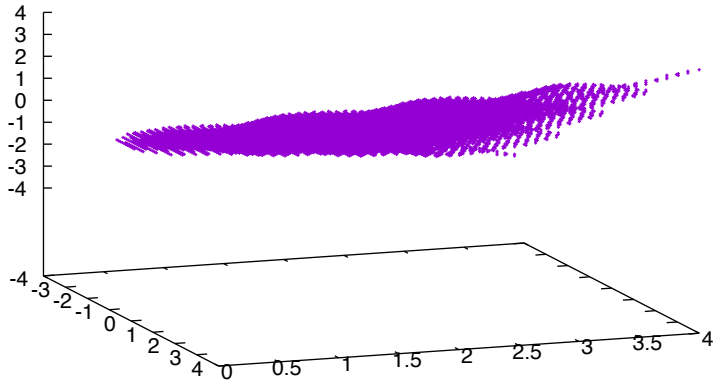
"A\_3\_4\_new" .



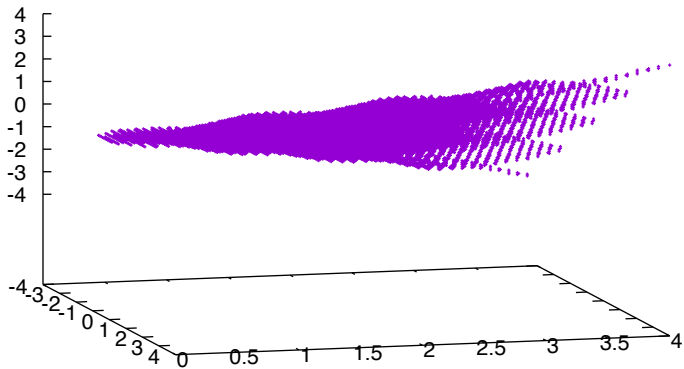
"A\_3\_4\_new" .



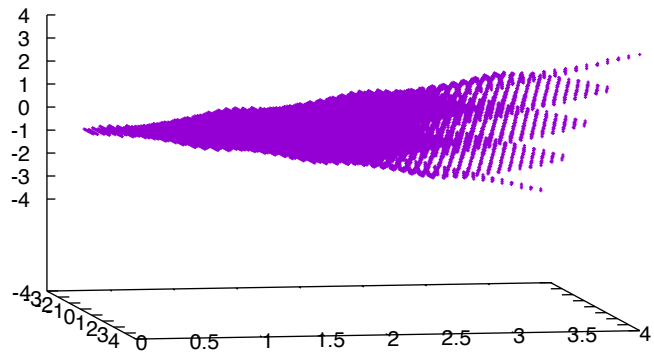
"A\_3\_4\_new" .



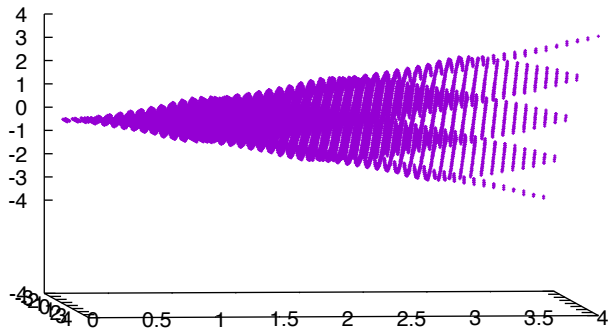
"A\_3\_4\_new" .



"A\_3\_4\_new" .

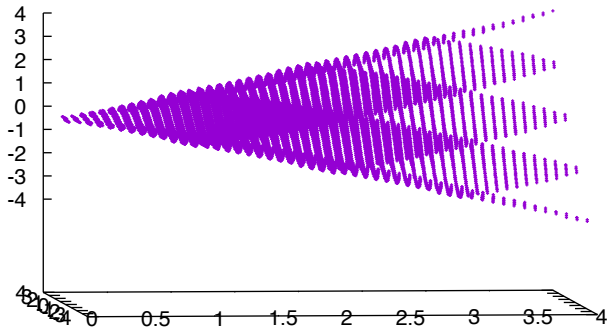


"A\_3\_4\_new" .

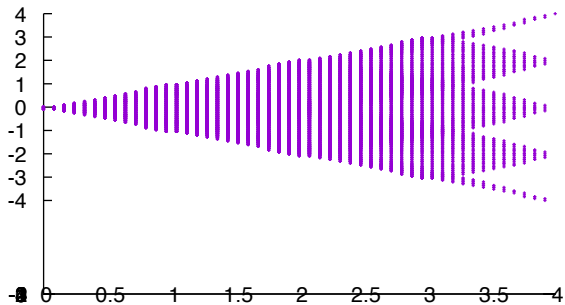




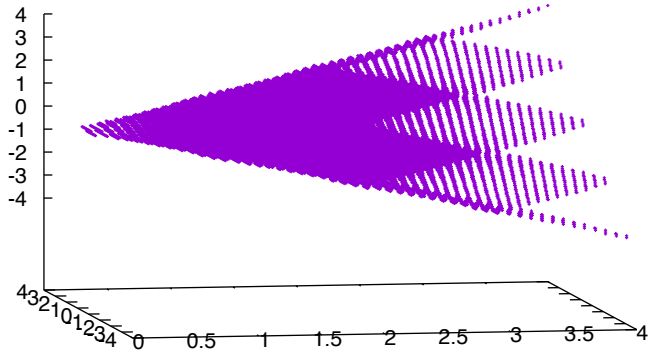
"A\_3\_4\_new" .



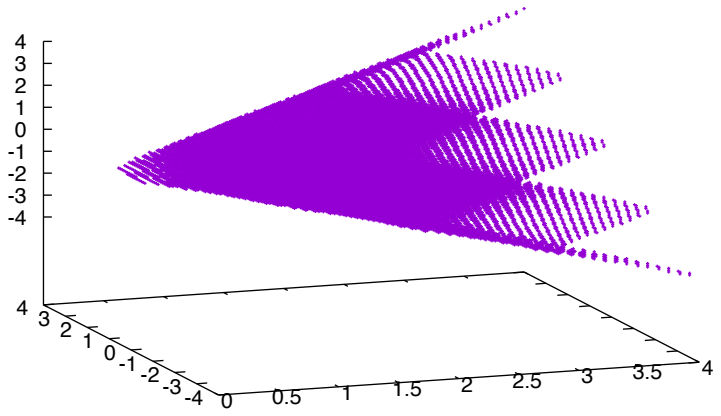
"A\_3\_4\_new" .



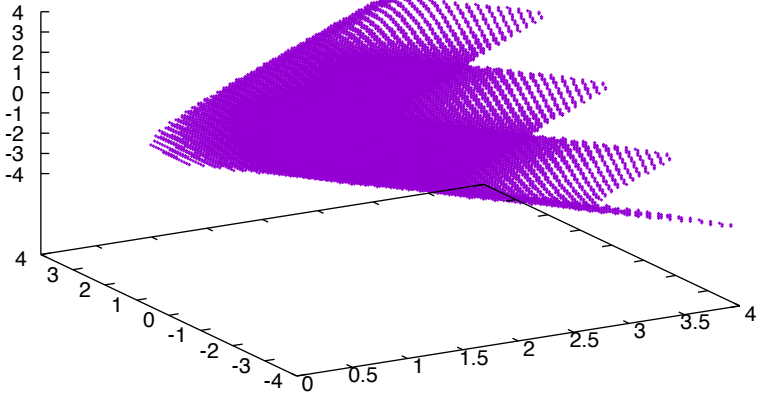
"A\_3\_4\_new" .



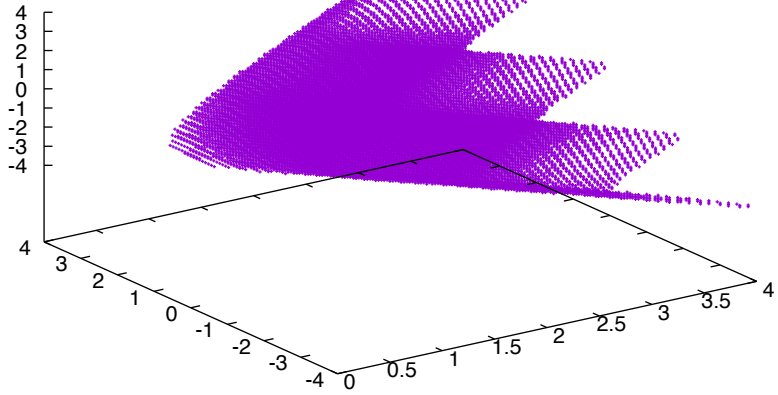
"A\_3\_4\_new" .



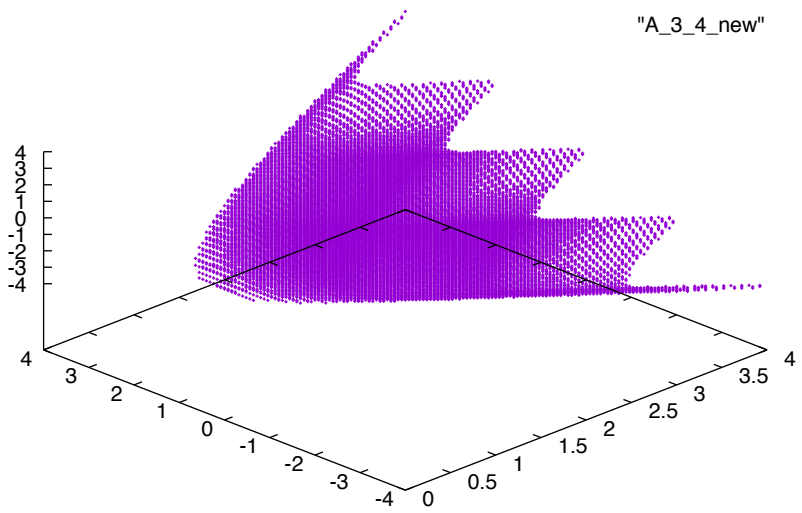
"A\_3\_4\_new" .



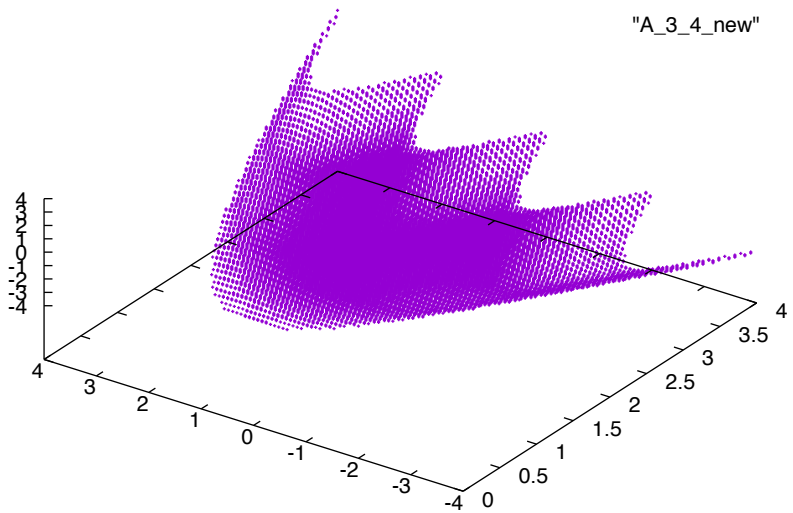
"A\_3\_4\_new" .



"A\_3\_4\_new" .

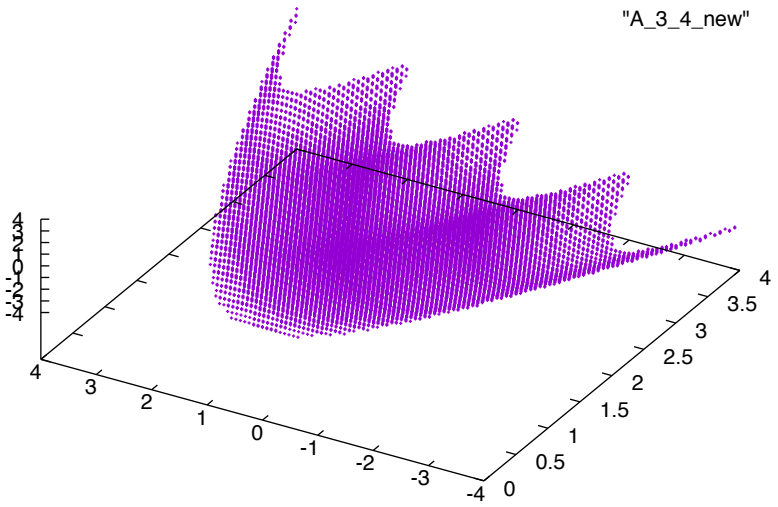


"A\_3\_4\_new" .

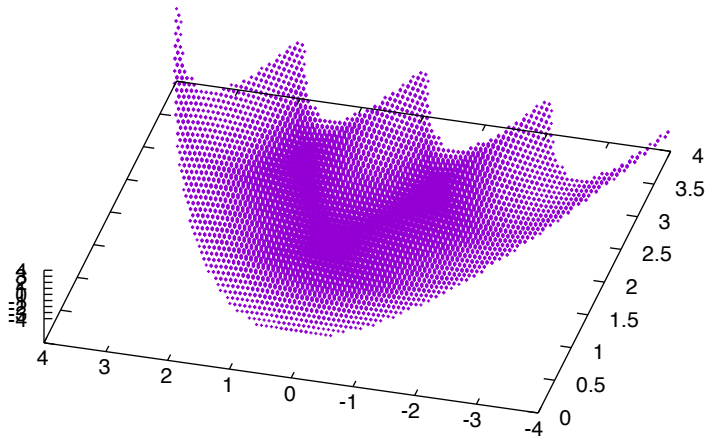




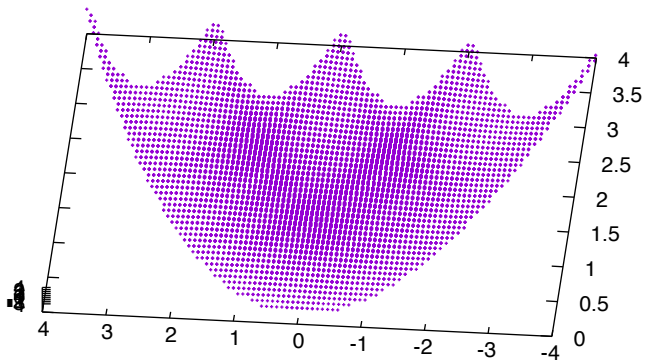
"A\_3\_4\_new" .



"A\_3\_4\_new" ·



"A\_3\_4\_new"



"A\_3\_4\_new"

